第 33 卷 第 4 期 计 算 机 工 程 2007 年 2 月
Vol.33 No.4 Computer Engineering February 2007
·工程应用技术与实现· 文章编号：1000—3428(2007)04—0233—03 文献标识码：A 中图分类号：TP393

基于磁盘和 SAN 的网络数据备份模型

熊 琦，王丽娜，王德军，赵大为
(武汉大学计算机学院，武汉 430079)

摘 要：构造了一个基于磁盘和存储区域网（SAN）的网络备份模型，阐述了该模型模块之间的通信机制，并使用安全套接层（SSL）保护备份数据的传输，在该模型中实现了差异备份的备份策略。
关键词：虚拟磁带库；数据备份；安全套接层；SAN；HDD

Network Data Backup Model Based on Hard Disk and SAN

XIONG Qi, WANG Lina, WANG Dejun, ZHAO Dawei
(School of Computer, Wuhan University, Wuhan 430079)

【Abstract】 A network data backup model based on hard disk (HDD) and storage area network (SAN) is constructed. The communicating mechanism is discussed, and the backup data is protected by secure socket layer (SSL). The differential backup is implemented in this model.
【Key words】 Virtual tape library(VTL); Data backup; Secure socket layer(SSL); Storage area network(SAN); Hard disk(HDD)

SAN[1]是一种类似传统局域网的高速存储网。它通过专用的网络连接设备实现备份操作的源端和目的端的直接连接。和普通的局域网相比，SAN不仅能支持远距离通信，还实现了大容量的集中存储，使存储成为一种共享的资源，并将存储设备网络从局域网中独立出来，从而有效地减轻了备份操作给局域网和备份服务器带来的负担，大大提高了备份执行期间局域网提供给客户的带宽和备份服务器的效率。

VTL[2]将磁盘和仿真软件结合起来，将磁盘虚拟成磁带库，使存储服务器对磁盘的操作如同操作一个磁带库一样。同传统的物理磁带库相比，虚拟磁带库不仅大大提高了备份速度以及数据存储的可靠性而且很好地保持同原有磁带备份环境的兼容性。另外随着磁盘价格的不断下跌，使用磁盘代替磁带作为备份介质的解决方案已经为越来越多的用户所接受。本文介绍了一个使用SAN技术的网络备份模型，并对该模型模块之间通信的实现做了较为详细的阐述。

1 网络备份模型

该网络备份模型[3]使用速度快、可靠性高的磁盘作为备份介质而使用成本较低的磁带库作为归档介质，由如下 4 部分组成。

(1)备份服务器：接受用户通过客户操作界面提交的任务，并作为整个备份系统的中枢监控所有的备份和恢复操作。

(2)应用服务器(备份客户端)：提供备份需要的文件属性和数据，并在恢复时将其写回。

(3)存储服务器：管理磁盘阵列和磁带库，负责对所管理的存储介质进行读写等相关操作，另外还自带虚拟磁带库模块模拟磁带库的方式操作磁盘。

(4)索引数据库：在备份时保存作业，存储介质以及文件索引等信息，以便恢复操作时能正确定位文件。

为了更高效地实现备份和恢复操作，本模型被分成如图 1 所示的 3 层结构：操作管理层，控制调度层和数据迁移层。其中模型系统结构的复杂程度和数据通信量从上往下逐渐增加。因为在备份系统中几乎超过 99%的数据通信量是备份数据的拷贝，而只有不到 1%的数据通信量为控制信息，所以将承担数据拷贝任务的数据迁移层放在具有高速传输能力的 SAN 中，大大提高了备份系统的效率。备份模型架构如图 1 所示。

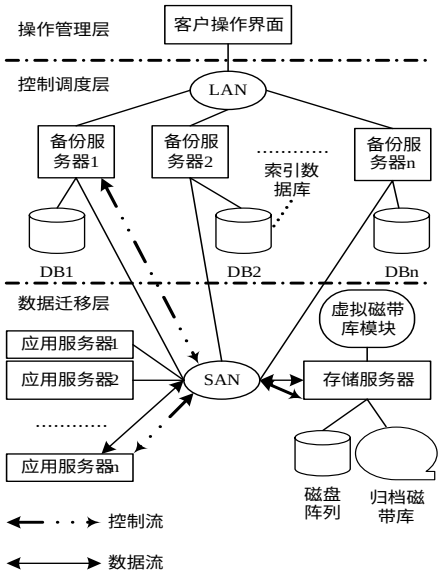

图 1 备份模型架构

2 模块间通信的实现

该系统模块之间使用TCP/IP协议进行通信，并遵循Server/Client模式[6]进行数据传输。模块之间的通信需求如图 2 所示。

基金项目：科技部中小企业创新基金资助项目(04C26214201280)；国家自然科学基金资助项目(60473023)
作者简介：熊 琦(1983－)，男，博士生，主研方向：网络存储；王丽娜，教授、博导；王德军，博士生；赵大为，硕士生
收稿日期：2006-02-23 **E-mail：**xq832001@126.com

系统中模块之间的通信类型分为两种：数据通信和消息通信。数据通信用来传输备份的数据，而消息通信是指模块之间的命令交互。在数据通信中传输的包被称为数据包，而在消息通信中传输的包则被称为消息包。

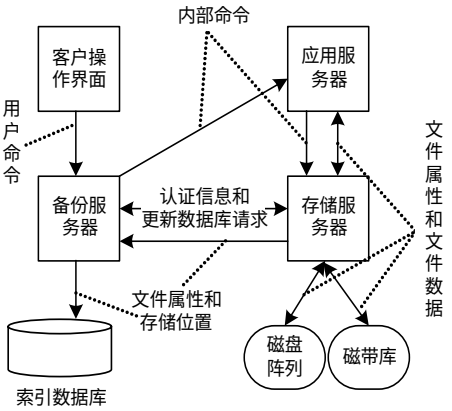

图 2 模块间的通信需求

2.1 数据包格式设计

本系统数据传输时使用的数据包又分为两种不同的类型：包头包和普通数据包

(1)包头包

具体形式如下所示：

<File-index>	<Stream-type>	0

<File-index>记录了本数据包所记录的文件在整个备份任务中所处位置的序号，这个序号从 1 开始并随着发送的文件数目增加而增加。

<Stream-type>表示紧跟着本包头包的普通数据包的内容：1 代表文件属性记录，2 代表文件数据。

包头包末尾的 0 是一个占位符号，没有什么特殊的意义。

(2)普通数据包

它跟在包头包后面，内容由前面的包头包指定，连续的普通数据包由一个空包结尾，表示后面可能是另外的一个包头包。

如果一次数据传输由一个内容为-1 的响应结束，则表示本次数据流已经传输完毕，需要接收方进行响应。

2.2 消息包格式设计

消息包又分为两种类型：命令包和响应包。

本系统模块间使用一种“命令－响应”模式进行通信并遵循以下规则：

(1)所有的控制信息都放在消息包中传输。

(2)命令使用 ASCII 码表示，所有的二进数据都必须转化为 ASCII 码。

(3)对于所有的响应包都预制了一个字符代码前缀，BS 代表此命令响应是备份服务器发出的，AS 代表是应用服务器(客户端)发出的，SS 代表是存储服务器发出的。

(4)服务器收到的任何没有字符代码前缀的响应包可以认为是来自网络另外一端的命令包，因为有时候通信的双方可以同时向对方发送命令。

(5)任何一个负数响应包都是要求通信的对方进行响应。

2.3 备份文件传输过程

图 3 显示了一个包括文件属性和文件数据在内的完整文件，在本系统中应用服务器和备份服务器之间的传输过程。在整个文件传输完毕后，备份服务器向应用服务器发送 BS OK 响应以确认刚才传输的文件。

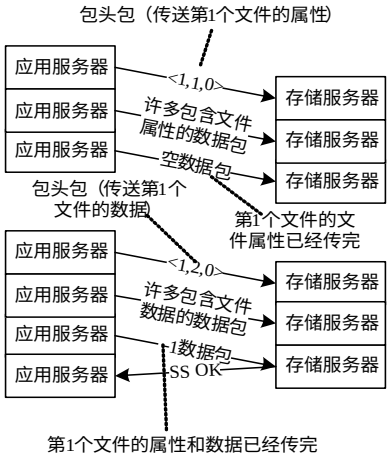

图 3 文件传输过程

2.4 数据传输加密的实现

备份和恢复过程中一个关键问题是如何保证所传输数据的安全性，如何防止数据在传输过程中被窃取或篡改。本系统中使用附加的安全模块实现了安全套接层(SSL)的功能，可有效地保护线路上所传输的数据。图 4 为加密通信实现过程。

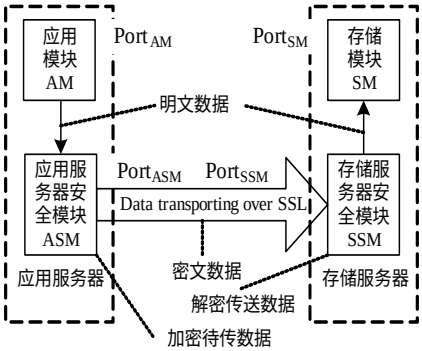

图 4 加密通信实现过程

安全模块分别运行在应用服务器和存储服务器上并监听 $Port_{ASM}$ 和 $Port_{SSM}$ 端口。另外应用模块(AM)和存储模块(SM)分别监听 $Port_{AM}$ 和 $Port_{SM}$ 端口，下面是安全通信的过程。

(1)应用服务器安全模块(ASM)同存储服务器安全模块(SSM)建立 SSL 连接。

ASM：发送“ASM Hello”发起握手，附带可用的加密算法表 $List_A$、随机数 R_A 以及自己的版本号 Ver_A，形式化表述为

$$ASM \rightarrow SSM : R_A; List_A; Ver_A$$

SSM：发送响应“SSM Hello”，附带本次通信使用的加密算法 E_S、自己的版本号 Ver_S 以及包含 SSM 对其公钥 K_S^+ 签名的证书 $Sign_{CA}^{SSM}(K_S^+)$。同时也提供一个随机数 R_B 用来产生密钥，其形式化表述为

$$SSM \rightarrow ASM : Ver_S; Sign_{CA}^{SSM}(K_S^+); E_S; R_B$$

ASM：对 SSM 发送过来的证书进行验证并从中获取其公钥，同时生成一个秘密消息($Secret_A$)，用 SSM 的公钥(K_S^+)对其加密后返回给 SSM，形式化表述为

$$ASM \rightarrow SSM : E\{Secret_A\}K_S^+$$

SSM：将收到的秘密消息用私钥(K_S^-)解密。会话密钥协商成功，双方可用同一会话密钥进行通信，形式化表述为

$$SSM \rightarrow ASM : D\{E\{Secret_A\}K_S^+\}K_S^-$$

(2)应用模块将数据发送到同时运行在应用服务器上的安全模块 ASM。

(3)ASM 将接收到的数据分成很多可管理的块,然后对这些数据块进行压缩、添加 MAC 信息、使用约定的加密算法加密，并对密文数据附加记录头形成传输的最小单位——记录块，最后将一系列记录块发送到存储服务器的 $Port_{SSM}$ 端口。

(4)SSM 监听到数据到达，接收数据并将其解密、校验、解压并重新组合成文件。

(5)SSM 将文件发送给 SM，SM 将其解密并存储到物理介质上，从而完成了本次数据传输。图 5 为加密过程。

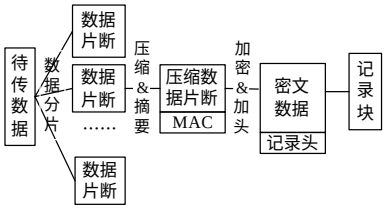

图 5 加密过程

3 备份和归档操作的实现

备份和归档是两个不同的概念。备份是为了保存近期日常数据的副本，以便在灾难发生后进行恢复，备份的保存期相对较短，但是要具备自动管理的能力。归档是为了保存阶段性总结，以便中长期备份或容灾，也可用于异地恢复，但是通常没有自动恢复的要求。

3.1 备份分类

(1)全备份[5]：将待备份数据整个备份。全备份的优点是方便、直观，当发生数据丢失的灾难时很容易就能恢复丢失的数据；缺点是数据冗余度大，存储空间浪费严重。

(2)增量备份：每次只备份相对于上一次备份后新增加的和修改过的数据。增量备份优点十分明显：没有重复地备份数据，既节省了存储空间，又缩短了备份时间；缺点在于发生灾难时恢复数据比较麻烦。

(3)差异备份[6]：每次只备份相对于上一次全备份后新增加的和修改过的数据。差异备份在很好地避免了前两种备份策略缺点的同时又具有它们的优点。

3.2 备份实现

在图 1 的模型基础上，采用第 2 节所描述的通信机制实现了差异备份的备份策略，其具体过程如下(其中备份服务器简称 BS，存储服务器简称 SS，应用服务器简称 AS)。

Step1 用户通过操作界面向备份服务器提交任务。

Step2 备份服务器同存储服务器的交互。

SS：进入监听状态。

BS：请求建立连接，同时发送自己的名字和口令进行认证。

SS：SS OK 通过身份认证，接受连接请求并建立连接。

BS：发送本次任务的任务编号、对存储介质的操作类型(读或写)以及要求使用的存储介质的名称和种类。

SS：SS OK 成功接收任务信息，并返回给备份服务器执行备份操作的授权凭证。

Step3 备份服务器同应用服务器的交互。

AS：进入监听状态。

BS：请求建立连接，同时发送自己的名字和口令进行认证。

AS：AS OK 通过身份认证，接受连接请求并建立连接。

BS：发送本次任务的任务编号以及存储服务器返回的操作授权凭证。

AS：AS OK 接收任务信息成功。

BS：发送存储服务器的 IP 地址、监听的端口以及本次任务可以使用的存储介质的名称和种类。

AS：AS OK 接收备份目的的信息成功。

BS：发送待备份的目录列表。

AS：AS OK 接收备份源的信息成功。

BS：发送备份种类(差异备份)。

AS：AS OK 接收备份种类成功。

AS：查询该备份源的全备份任务编号。

BS：BS OK 发送全备份任务编号。

AS：AS OK 接收编号成功。

AS：计算待备份文件的 hash 值，并随全备份任务编号一起发送到备份服务器请求验证是否在此任务中已经备份。

BS：BS OK 返回未备份文件列表。

AS：AS OK 接收列表成功。

Step4 应用服务器向存储服务器传输备份数据。

SS：进入监听状态。

AS：请求建立连接，同时发送待执行的任务编号及该任务的授权凭证。

SS：SS OK 接受请求，建立连接。

AS：传输备份数据。

SS：接收备份数据并写入物理介质。

AS：数据传输完毕。

SS：SS OK 接收数据成功。

Step5 存储服务器向备份服务器返回此次备份操作的信息。

SS：发送本次任务的编号、写入的存储介质编号、任务的起始和结束文件编号以及该介质最后被写入的时间。

BS：BS OK 接收任务信息成功,将信息写入索引数据库。

Step6 备份服务器通过操作界面向用户返回本次任务执行的信息。

3.3 归档实现

由于本系统使用了软件虚拟磁带库模块将磁盘阵列模拟成磁带进行操作，因此归档操作只是虚拟磁带和物理磁带之间的拷贝，在此不作赘述。

4 结语

本文给出了一个基于磁盘并引入 SAN 技术的网络数据备份模型，在此基础上详细给出了备份模型模块之间通信协议的设计，并且实现了对数据传输信道的加密，有效地保护了备份数据的安全，最后给出了差异备份的实现过程。在实际工作中，可以参照该模型设计符合需要的备份恢复系统。

参考文献

1 Kochut A, Bobroff N, Beaty K, et al. Management Issues in Storage Area Networks[C]//Proc. of Network Operations and Management Symposium. 2004: 453-466.

2 CA Corp. BrightStor CA-Vtape product Description[Z]. 2002. http://www3.ca.com/Files/Datasheets/Vtape_pdf.pdf.

3 Sibbald K, Walker J. Development Manual of Bacula[Z]. 2004. http://www.bacula.org/dev-bacula.pdf.

4 Khattar R. Introduction to Storage Area Network[M]. Redbooks Pulications, 1999.

5 Freier O, Karlton P, Kocher C. The SSL Protocol Version 3.0[Z]. 2002. http://wp.netscape.com/eng/ssl3/draft302.txt.

(下转第 238 页)